神戸市道路公社
情報セキュリティポリシー

制定日：平成２２年２月１日
改正日：令和６年１月１５日

神戸市道路公社

改訂履歴

施行年月日	版番号	改訂理由・内容
平成 22 年２月１日	第 1.0 版	初版発行
平成 25 年４月１日	第 1.1 版	職制改正に伴う一部改正
令和 ４年４月１日	第 1.2 版	職制改正に伴う一部改正
令和５年４月１日	第 1.3 版	有期雇用職員就業規則改正に伴う一部改正
令和６年１月 15 日	第 1.4 版	執務室外の情報処理作業の制限の一部改正

目　　次

１．目的

本公社において保有する情報資産は、常にさまざまな脅威にさらされていることを強く認識し、個人情報をはじめとする重要な情報資産の安全確保を徹底するとともに、積極的な情報開示に取り組むことにより、お客さま及び社会との信頼関係を一層ゆるぎないものとする必要がある。

そのため、本公社の情報資産の機密性、完全性及び可用性を維持するための対策を整備するために神戸市道路公社情報セキュリティポリシー（以下「情報セキュリティポリシー」という）を定める。

２．定義

（１）ネットワーク

コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。

（２）情報システム

ハードウェア、ソフトウェア、ネットワーク等で構成され、情報処理を行う仕組みをいう。

（３）情報資産

情報システム及びネットワークにより処理、保管、通信、送付されるすべての情報をいう。

（４）情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（５）機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（６）完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（７）可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

３．情報セキュリティポリシーの適用範囲

（１）組織の範囲

経営企画部及び道路管理部とする。

（２）情報資産の範囲

情報セキュリティポリシーが対象とする情報資産は次のとおりとする。ただし、ETC に関する情報資産、神戸市土木積算システム及び設備積算システムに関する情報資産については、別の定めに基づきセキュリティ対策を実施するものとし、これらの情報資産については、本セキュリティポリシーの対象から除くものとする。

①物理資産

コンピュータ・ネットワーク・記録媒体等物理的な形状を有する資産であり、かつ情報を利用するのに必要な資産

②データ資産

データ及び情報システムの設計等に関する情報

③ソフトウェア資産

コンピュータ等の情報機器において稼動するプログラム

④サービス資産

電源、メールサービス等契約により提供される情報システムに関連する業務

４．職員等の義務

役員、職員（再任用職員を含む。以下同じ）、有期雇用職員及び委託業務等従事者（以下「職員等情報取扱者」という。）は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行にあたっては情報セキュリティポリシーを遵守するものとする。

また、人材派遣職員に業務を行わせる場合においても、本ポリシーを遵守させるものとする。

５．管理体制及び権限と責任

本公社の情報資産について、適切に情報セキュリティ対策を推進・管理するための組織体制を確立するものとする。そのために次に掲げるものを置く。

（１）情報セキュリティ最高責任者（経営企画担当常務理事）

情報セキュリティ最高責任者は、情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

（２）情報セキュリティ統括責任者（経営企画課長）

情報セキュリティ統括責任者は、情報セキュリティ最高責任者を補佐するとともに、本公社のすべての情報資産における情報セキュリティ対策に関する統括的な権限及び責任を有する。また、情報管理者に対して情報セキュリティ対策に関する指導及び助言を行う権限を有する。

（３）情報管理者（各課長）

情報管理者は、課内における情報資産の情報セキュリティ対策及び当該システムにおける開発、設定の変更、運用、見直し対策等を行う権限及び責任を有する。

（４）情報セキュリティ監査統括責任者（経営企画課長）

情報セキュリティ監査統括責任者は、情報セキュリティ監査の計画、実施、報告等を行う権限及び責任を有する。

（５）情報化推進会議

情報セキュリティ統括責任者及び情報管理者により構成され、情報セキュリティに関する重要な事項を審議する。

情報化推進会議の事務局は、経営企画課に置く。

６．情報資産への脅威

情報セキュリティ対策を講じるうえでは、情報資産に対する脅威の発生度合いや発生した場合の影響を考慮するものとする。特に次の脅威については、十分な措置を講じるものとする。

（1）部外者による不正アクセス又は不正操作によるデータやプログラムの持ち出し・盗聴・改ざん・消去、機器及び媒体の盗難等

（2）職員等情報取扱者による意図しない操作、不正アクセス又は不正操作によるデータやプログラムの持ち出し・盗聴・改ざん・消去、機器及び媒体の盗難、規定外の端末接続によるデータ漏えい等

（3）地震、落雷、火災等の災害、事故、故障等によるサービス及び業務の停止

7．情報資産の分類及び管理

（1）情報資産の分類

対象となる情報資産は、各々の情報資産の機密性、完全性及び可用性を踏まえセキュリティ対策を講じるものとする。

また、重要な情報資産は以下のものとする。

	定　　義
機密性	・個人情報に関するデータ ・法令の規定により秘密を守る義務を課されているデータ ・部外に知られることが適当でない法人その他団体に関するデータ ・部外に漏れた場合に道路公社の信頼を著しく害するおそれのあるデータ ・公開することでセキュリティ侵害が生じるおそれがあるデータ
完全性	・個人情報に関するデータ ・法令の規定により秘密を守る義務を課されているデータ ・部外に知られることが適当でない法人その他団体に関するデータ ・部外に漏れた場合に道路公社の信頼を著しく害するおそれのあるデータ
可用性	・滅失しまたは損傷した場合、その復元が著しく困難であるため道路公社の円滑な運営が妨げられるおそれのあるデータ

（2）情報資産の管理方法

① 情報資産の管理

ア 情報資産について、第三者が重要性の識別を容易に認識できないよう適切な管理を行わなければならない。

イ 全ての情報資産を明確に識別し、重要な情報資産に対しては必要に応じて目録を作成して管理しなければならない。

② データの作成

ア 業務上必要のないデータを作成してはならない。

イ 作成途上のデータについても、紛失や流出を防止しなければならない。また、データの作成途上で不要になった場合は、当該データを消去しなければならない。

③ 情報資産の利用

ア 情報資産を利用する者は、情報資産を業務上の目的以外に利用してはならない。

④ 情報資産の廃棄

ア　記録媒体が不要となった場合は、当該媒体に含まれるデータの消去を行ったうえで焼却、裁断、溶解等により復元不可能な状態にして廃棄しなければならない。

８．情報セキュリティ対策

情報資産に対する脅威から情報資産を保護するため、次の情報セキュリティ対策を講ずるものとする。

（１）物理的セキュリティ対策

コンピュータ設置場所への入退室、サーバ等の管理、通信回線及び端末等への物理的な対策を講じる。

（２）人的セキュリティ対策

情報セキュリティに関し、職員等情報取扱者が遵守すべき事項を定めるとともに、研修・訓練及び啓発を実施するなど人的な対策を講じる。

（３）技術的セキュリティ対策

コンピュータ等の管理、アクセス制御、コンピュータウイルス等不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（４）運用面のセキュリティ対策

情報システムに関し、情報セキュリティポリシーの遵守状況の確認等、情報セキュリティポリシーの運用面の対策を講じる。

９．物理的セキュリティ対策

（１）サーバ等の管理

①　入退室の管理

ア　情報管理者は、重要な情報資産データが記録されている記録媒体の保管場所及びそれを取り扱うコンピュータ設置場所の入退室について、適正な管理を行わなければならない。

イ　外部からの訪問者が管理区域に入室する場合には、職員の承諾を必要とするものとする。

②　装置の取り付け等

サーバの設置に際しては、温度、湿度等の環境条件を十分留意したサーバ室又は固定式ラックを用いるなど地震にも耐えられるような対策を施さなければならない。

③　電源

サーバ等の機器の電源については、落雷等による過電流対策を施し、当該機器を正常に停止するまでの間に十分電力を供給できる容量の予備電源を備え付けなければならない。

④　機器等の定期保守及び修理

ア　サーバ等の機器は、必要に応じ保守点検を実施しなければならない。

イ　記憶装置を内蔵する機器を外部の業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、修理を委託する事業者との間で、守秘義務契約を締結するなど秘密保持体制の確認を行わせなければならない。

⑤　機器の廃棄等

機器を廃棄、リース返却等を行う場合、機器内部の記憶装置から全てのデータを消去のうえ、復元不可能な状態にする措置を施さなければならない。

（2）ネットワークの管理

ネットワークに使用する回線は、送信途上においてデータの破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策が実施されたものでなければならない。

10. 人的セキュリティ対策

（1）職員等の責務

①　情報セキュリティポリシー等の遵守義務

職員等情報取扱者は、情報セキュリティポリシー及びこれに基づく文書に定められている事項を遵守し、情報システム及び情報資産を適切に管理しなければならない。

②　法令等の遵守義務

職員等情報取扱者は、職務の遂行において使用する情報資産を保護するために、法令等を遵守し、これに従わなければならない。

③　個人所有の情報資産の持ち込み禁止

職員等情報取扱者は、個人の所有するパーソナルコンピュータ及び記録媒体等の持ち込みをしてはならない。

④　情報資産の持ち出し等の禁止

職員等情報取扱者は重要な情報資産を公社外へ持ち出してはならない。ただし、合理的理由のある場合、かつ情報管理者等管理権限のある者の許可を得た場合に限り、公社外への持ち出しができるものとする。

⑤　業務目的外の利用禁止

職員等情報取扱者は、業務目的外でのパーソナルコンピュータ等の利用、情報システムへのアクセス、電子メールの利用及びインターネットへのアクセス等を行ってはならない。

⑥　端末等の利用

ア　職員等情報取扱者は、端末のソフトウェアに関するセキュリティ機能の設定を情報管理者の許可なく変更してはならない。

イ　職員等情報取扱者は、端末や記録媒体、データが印刷された文書等について、第三者に使用されること、又は情報管理者等管理権限のある者の許可なく情報を閲覧されることがないように、離席時の端末のロックや記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

⑦　執務室外における情報処理作業の制限

ア　職員等情報取扱者は、執務室外で情報処理作業を行う場合には、情報管理者等管理権限のある者の許可を得なければならない。

イ　職員等情報取扱者は、執務室外で情報処理作業を行う際、情報管理者の許可を得た場合を除き、執務室内で使用しているパーソナルコンピュータ、個人の所有するパーソナルコンピュータその他の端末(タブレット端末やスマートフォン)又は貸出用端末によ

る情報処理を行ってはならない。ただし、情報管理者の許可を得て当該端末を利用する場合において、公社の管理するネットワークにアクセスするときは、情報セキュリティ統括責任者が許可した専用回線同等の通信手段によるものに限る。

⑧　異動、退職時等の遵守事項

職員等情報取扱者は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

（2）研修

全ての職員等情報取扱者は、情報セキュリティに関する意識を深め情報セキュリティ上の問題が生じないようにするため、定められた研修に参加しなければならない。

（3）事故等の報告・分析等

①　事故等の報告

ア　職員等情報取扱者は、情報セキュリティに関する事件・事故、システム上の欠陥及び誤動作を発見した場合、若しくは外部から報告を受けた場合、速やかに情報管理者等権限のある者に報告しなければならない。

イ　報告を受けた情報管理者等権限のある者は、速やかに情報セキュリティ統括責任者に報告しなければならない。

ウ　情報セキュリティ統括責任者は、報告のあった事故等について、必要に応じて、情報セキュリティ最高責任者に報告しなければならない。

②　事故等の分析・記録等

事故等を引き起こした部門の情報管理者は、情報セキュリティ統括責任者と連携し、これらの事故等を分析し、記録を保存しなければならない。

（4）パスワードの管理

①　職員等情報取扱者は、自己のパスワードに関し、次の事項を遵守しなければならない。

ア　パスワードは秘密にし、パスワードの照会等には一切応じない。

イ　情報システム又はパスワードに対する危険のおそれがある場合には、情報管理者等権限のある者に速やかに報告し、パスワードを速やかに変更する。

ウ　複数の情報システムを扱う場合は、同一のパスワードを複数のシステムで用いない。

エ　職員等情報取扱者の間でパスワードを共有しない。

（5）外部委託に関する管理

①　契約書の記載事項

駐車場管理業務、有料道路付帯設備等維持管理業務、料金徴収業務など、ネットワーク及び情報システムの開発・保守並びにデータ処理その他情報処理に係る業務を外部委託する場合は、当該委託先事業者との間で、下記事項を明記した契約を締結しなければならない。

ア　データその他業務上知り得た情報（以下「データ等」という）の秘密の保持に関する事項

イ　第三者への委託の禁止又は制限に関する事項

ウ　データ等の目的以外の目的のための使用及び第三者への提供の禁止に関する事項
エ　データ等の複写及び複製の禁止に関する事項
オ　データ等の取扱いに関する事故の発生時における報告義務に関する事項
カ　契約に違反した場合における契約の解除及び損害賠償に関する事項
キ　委託業務終了時の資産の返還、廃棄等に関する事項
ク　情報セキュリティポリシー及びこれに基づく文書の遵守に関する事項
ケ　委託先の責任者、委託内容、作業者、作業場所の特定に関する事項

11. 技術的セキュリティ対策

（1）コンピュータ及びネットワークの管理

① ファイルサーバの設定等

データを共有するためのファイルサーバを設置する場合に、特定の職員のみが取扱う権限を持つデータについては、同一所属であっても、権限のない者が閲覧及び使用できないよう設定しなければならない。

② 情報資産のバックアップ

職員等情報取扱者は、必要なものはサーバの二重化対策実施の有無に関わらず、定期的に情報資産のバックアップを行うものとする。

③ Ｗｅｂサイトでの情報公開時の注意事項

Ｗｅｂサイトにより情報を公開・提供する場合に、当該サイトに係るシステムにおいての情報の漏えい・改ざん・消去などを防止しなければならない。

④ 無線ＬＡＮの利用禁止

公社の管理するネットワークにおいて、無線ＬＡＮを利用した接続又は端末等の無線機能を利用した端末間通信を行ってはならない。

⑤ 無許可ソフトウェアの導入等の禁止

ア　職員等情報取扱者は、各自に供与された端末に対して、情報セキュリティ統括責任者が定めるもの以外のソフトウェアの導入を行ってはならない。ただし、業務を円滑に遂行するために必要なソフトウェアについては、情報セキュリティ統括責任者の許可を得た場合に限り、利用することができる。

イ　職員等情報取扱者は、不正にコピーしたソフトウェアを導入又は使用してはならない。

⑥ 電子メール

ア　メールアドレス保有者は、業務上必要のない送信先に電子メールを送信してはならない。

イ　メールアドレス保有者は、複数の宛先に電子メールを送信する場合、必要がある場合を除き他の送信先の電子メールアドレスがわからないようにしなければならない。

ウ　メールアドレス保有者は、重要な電子メールを送信する場合、誤送信がないよう注意し、誤送信した場合には、情報管理者に報告しなければならない。

⑦ 無許可端末の接続禁止

職員等情報取扱者は、情報管理者等権限のある者の許可なく端末等をネットワークに接続してはならない。

（2）アクセス制御

① 所管するネットワークに権限がない職員等情報取扱者がアクセスすることが不可能となるように適切な対応を行わなければならない。

② ネットワークにおけるアクセス制御

ネットワークサービスを利用する権限を有しない職員等情報取扱者が当該サービスを利用できるようにしてはならない。

③ 外部からのアクセス

情報セキュリティ統括責任者は外部から公社のネットワークにアクセスさせるときは原則として外部に公開されているサーバに対してのみ行わせるものとし、直接内部ネットワークにアクセスすることを許可してはならない。

（3）システム開発、導入、保守等

① 情報システムの調達

情報セキュリティ統括責任者は、情報システムの調達にあたっては、一般に公開する調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

② 情報システムの開発等

情報セキュリティ統括管理者は、ネットワーク及び情報システムの開発、導入、更新及び運用保守にあたっては、次の事項を定める。

ア 責任者及び監督者

イ 作業者及び作業範囲

ウ 開発するシステムと運用中のシステムとの分離

エ 開発・保守に関する設計仕様などの成果物の提出

オ セキュリティ上問題となり得るおそれのあるハードウェア及びソフトウェアの使用禁止

カ アクセス制限

キ 機器の搬入出の際の許可及び確認

ク 記録の提出義務

ケ 仕様書・マニュアル等の定められた場所への保管

③ 情報システムの移行

ア システム開発・保守計画の策定時に、情報システムの移行手順を明確にしなければならない。また、移行の際、情報システムに記録されているデータの保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるように配慮しなければならない。

イ 新たに情報システムを導入する際には、すでに稼動している情報システムに接続する前に、十分な試験を行わなければならない。また、既存の情報システムを更新する際は、すでに稼動している情報システムとの連携について、十分な試験を行わなければならない。

④ ソフトウェアの保守及び更新

ソフトウェア等を更新、又は修正プログラムを導入する場合、不具合及び他のシステムとの相性の確認を行い、計画的に更新し、又は導入しなければならない。

（4）コンピュータウイルス等不正プログラム対策

① 情報セキュリティ統括責任者の実施事項

ア コンピュータウイルス等の情報について職員等情報取扱者に対する注意喚起を行う。

イ コンピュータウイルス等に関する情報収集に努める。

ウ コンピュータウイルス等対策ソフトウェア及び定義ファイルは常に最新のものとする。

② 情報管理者等の実施事項

ア 所管するサーバ及び端末に、コンピュータウイルス等対策ソフトウェアを常駐させる。

イ コンピュータウイルス等対策ソフトウェア及び定義ファイルは常に最新のものに保つ。また、インターネットに接続していないシステムにおいても、定期的に当該ソフトウェア及び定義ファイルの更新を行う。

③ 職員等情報取扱者の遵守事項

ア 端末において、コンピュータウイルス等対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更しない。

イ 外部ネットワーク及びフロッピィディスク等の記録媒体からデータ又はソフトウェアを取り入れる際には、必ずコンピュータウイルス等対策ソフトウェアによるチェックを行う。

ウ 外部ネットワーク及びフロッピィディスク等への記録媒体へデータ又はソフトウェアを送信・書き込みする際には、必ずコンピュータウイルス等対策ソフトウェアによるチェックを行う。

エ 差出人が不明な電子メール又は不自然なファイルが添付された電子メールを受信した場合は速やかに削除する。

オ 端末に対してコンピュータウイルス等対策ソフトウェアによる完全スキャンを定期的に行い、スキャンの実行を途中で止めない。

カ 添付ファイルのあるメールを送受信する場合は、コンピュータウイルス等対策ソフトウェアでチェックを行う。

キ コンピュータウイルス等に感染した場合は、ＬＡＮケーブルの即時取り外し又は機器の電源遮断を行う。

（5）不正アクセス対策

① 不正アクセス防止

情報セキュリティ統括責任者及び情報管理者は、不正なアクセスによる影響を防止するための必要な措置を講じなければならない。

ア 不正アクセスによるデータの書換えを検出し、Ｗｅｂサイトの改ざんを防止する。

イ ソフトウェアにセキュリティホールが発見された場合は、速やかに修正プログラムを適用する。

② 記録の保存

情報セキュリティ最高責任者及び情報セキュリティ統括責任者は、不正アクセス行為の禁止等に関する法律違反等犯罪の可能性がある不正アクセスを受けた場合、不正アクセスの記録の保存に努めるとともに、警察・関係機関との緊密な連携に努めなけ

ればならない。

12. 運用面のセキュリティ対策

（1）情報セキュリティポリシー等の遵守状況の確認及び対処

情報管理者は、所管の範囲において情報セキュリティポリシー及びこれに基づく文書の遵守状況について確認を行い、問題を認めた場合には速やかに情報セキュリティ統括責任者に報告しなければならない。情報セキュリティ統括責任者は、発生した問題について適切かつ速やかに対処しなければならない。

（2）運用管理における留意点

① セキュリティポリシー等の閲覧

情報セキュリティ統括責任者及び情報管理者は、職員等情報取扱者が常に情報セキュリティポリシー及びこれに基づく文書を参照できるよう配慮しなければならない。

② 職員等情報取扱者の報告義務

職員等情報取扱者は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに情報管理者に報告を行わなければならない。

（3）緊急時の対応

情報資産への重大な侵害が発生した場合又は発生する恐れがある場合において、連絡・証拠保全・被害拡大の防止・復旧・再発防止等を迅速かつ適切に実施しなければならない。

13. 情報セキュリティポリシー等に関する違反に対する対応

（1）懲戒処分

情報セキュリティポリシー及びこれに基づく文書に違反した職員等情報取扱者並びにその監督責任者は、その重大性、発生した事象の状況等に応じて、懲戒処分の対象となる。

（2）再発防止の指導等

職員等情報取扱者に情報セキュリティポリシー等に違反する行為がみられた場合には、情報セキュリティ統括責任者、情報責任者は、速やかに次の措置を講じなければならない。

① 当該職員等情報取扱者に対して違反行為の事実を通知し、再発防止の指導その他適切な措置を行う。

② 指導等によっても改善されない場合、当該職員等情報取扱者の情報資産の使用権を停止あるいは剥奪する。

③ 違反行為が生じた場合、違反行為の内容、指導内容その他措置の状況について情報セキュリティ統括責任者に報告する。

14. 評価・改善・見直し

（1）監査

① 実施方法

情報セキュリティ最高責任者は、情報セキュリティ監査統括責任者に命じ、情報セ

キュリティ対策状況について、定期的及び必要に応じて監査を行わせなければならない。

② 監査結果の報告

情報セキュリティ監査統括責任者は、監査結果を情報化推進会議に報告しなければならない。

③ 監査調書等の保管

情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を適切に保管しなければならない。

④ 指摘事項への対処

情報セキュリティ統括責任者は、監査結果を踏まえ、指摘事項に関係する情報管理者等に対し、当該事項への対処を指示しなければならない。また、指摘事項に関係しない情報管理者等に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

（2）自己点検

① 実施方法

情報管理者は、所管するネットワーク及び情報システムの情報セキュリティ対策状況について、定期的及び必要に応じて自己点検を実施しなければならない。

② 自己点検結果等の報告

ア 情報管理者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティ統括責任者に報告しなければならない。

イ 情報セキュリティ統括責任者は、報告を受けた点検結果及び改善策を情報化推進会議に報告しなければならない。

③ 自己点検結果の活用

ア 職員等情報取扱者は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

イ 情報セキュリティ最高責任者は、情報セキュリティポリシー等情報セキュリティ対策の見直し時に点検結果を活用しなければならない。

（3）改善

① 是正措置

情報管理者は、業務上発見された問題、監査及び自己点検において指摘された問題等に対する再発防止のため、その原因を除去するための措置を施さなければならない。

② 予防措置

情報管理者は、業務上予見される問題、他の組織で発生したものと同種の情報セキュリティ事件・事故、監査及び自己点検において指摘されうる問題等の発生を未然に防止するため、その原因を除去するための措置を施さなければならない。

（4）情報セキュリティポリシーの見直し

情報セキュリティ最高責任者は、監査及び自己点検の結果、改善の状況、残留リスク、情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシーに

対して必要があると認めた場合その見直しを行う。